UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/589,837	08/18/2006	Frederic Beun	MM6019PCT	2806

79681   7590   11/18/2009

David A. Einhorn, Esq.
Baker & Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111

EXAMINER
VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
11/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _02 October 2009_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1,4-8,10-18 and 21-53_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1,4-8, 10-18 and 21-53_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/2/09 has been entered.

Claims 2-3 and 9 have been cancelled. Claims 1, 4-8, 10-18, and 21-53 are pending.

Response to Amendment

Claim Objections

Claim 1 is objected to because of the following informalities:

There is a misspelled word: "verity".

Claim 33 is objected to because this phrase in the preamble is unclear: "with said decoder in comprising means responsive to said processing algorithm for executing orders sent by the operator for".

Claim 36 is objected to because conditional access control cards are referred to as both "access control card" and "control cards". The terminology should remain consistent.

Claim Rejections - 35 USC § 101

Previous 101 rejections are withdrawn due to amendments.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 21-23 and 48-53 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 21-23 and 48-53, saying a message is in the format of source code is indefinite. The source is dependent on a loop which makes its impossible to determine the scope of the message. Secondly, messages are interpreted as having data, so it raises the question of why the message consists of source code. Source code when executed can create a message but saying the message consists of a source code format has no meaning. At the very broadest, a message format can consist of bit fields of various length but it cannot consist of a 'for loop'. Appropriate correction is required.

Response to Arguments

Applicant's arguments filed 8/3/09 have been fully considered but they are not

persuasive.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 4-8, 10-18, and 21-53 are rejected under 35 U.S.C. 102(b) as being

anticipated by USP 6,405,369, to Tsuria.

As per claim 1, Tsuria teaches a method for an operator to dynamically and

remotely control the pairing of digital data reception equipment (2) with one or more

external security modules (6, 8) each having a unique identifier (col. 3, lines 3-15) and

with each security module being adapted to cooperate with said digital data reception

equipment for controlling reception of distributed data by means of said digital data

reception equipment and with the digital data reception equipment having a computer

and stored program [decoder and programmed for activation; col. 7, lines 35-38],

method comprising the following steps (col. 1, lines 54-65):

using the computer the computer to verify whether or not the identifier of said

external security modules is memorized in the digital data reception equipment upon

connection of said external security modules to the digital data reception equipment

[second card is inserted in to the receiver to validate and identify the signature of said

second card; col. 7, lines 44-53],

if the unique identifier of the external security modules is memorized in the digital

data reception equipment, transmitting a control signal to the digital data reception

equipment defining configuration parameters to activate the pairing of the said digital

data reception equipment with said external security modules [chaining data; col. 7,

lines 45-48];

if the unique identifier of the external security modules is not memorized in the

digital data reception equipment, transmitting a control signal to the digital data

reception equipment defining configuration parameters to deactivate the pairing of the

said digital data reception equipment with said external security modules [inherent that if

the smart card's signature is not validated, there will be no pairing; col. 7, lines 45-48].

As per claim 4, Tsuria teaches at least one of the following set values: - authorize

memorization, - prohibit memorization, - erase identifiers previously memorized in the

reception equipment (2), - activate or deactivating the check phase (col. 3, lines 27-31)

including a procedure consisting of disturbing the data processing if the identifier of the

connected external security module (6, 8) is not previously memorized in the reception

equipment (col. 5, lines 10-15).

As per claim 5, Tsuria teaches that said signal also includes the maximum

allowable number of memorized identifiers (col. 9, lines 5-8).

As per claim 6, Tsuria teaches signal includes a reconfiguration set value through

which an updated list of identifiers of external security modules (6, 8) matched with the

reception equipment(2) is transmitted to said reception equipment (col. 7, lines 29-35).

As per claim 7, Tsuria teaches list is transmitted directly to the reception

equipment (col. 6, lines 55-59).

As per claim 8, Tsuria teaches list is transmitted through an external security

module (6, 8) connected to said reception equipment (col. 6, lines 40-45).

As per claim 10, Tsuria teaches data are distributed without encryption or

scrambled by an encrypted control word and in that each external security module (6, 8)

includes access rights to said data and a decryption algorithm for said control word (col.

5, line s35-40).

As per claim 11, Tsuria teaches said signal is transmitted to a reception

equipment (2) in an EMM message specific to an 25 external security module (6, 8)

associated with this reception equipment (col. 6, lines 55-60).

As per claim 12, Tsuria teaches a signal is transmitted to a reception equipment

(2) in an EMM message specific to this reception equipment (col. 6, lines 55-60).

As per claim 13, Tsuria teaches a given reception equipment (2) said list is transmitted in an EMM message specific to a security module (6, 8) associated with this reception equipment (col. 6, lines 55-60).

As per claim 14, Tsuria teaches a signal is transmitted to a group of reception equipment (2) in an EMM message specific to a group of external security modules (6, 8) associated with said reception equipment (col. 6, lines 55-60).

As per claim 15, Tsuria teaches signal is transmitted to a group of reception equipment (2) in an EMM message specific to said group of reception equipment (col. 6, lines 55-60).

As per claim 16, Tsuria teaches a given group of reception equipment (2), said list is transmitted in an EMM message specific to a group of external security modules (6, 8) associated with said reception equipment (col. 6, lines 55-60).

As per claim 17, Tsuria teaches said check signal is transmitted in a private flow processed by a dedicated software executable in each reception equipment as a function of the identifier of the external security module associated with said reception equipment (col. 6, lines 55-60).

As per claim 18, Tsuria teaches a given group of reception equipment (2), said list is transmitted in a private flow to each reception equipment (col. 6, lines 55-60).

As per claims 21, 22, and 23, Tsuria teaches EMM are formatted to convey to the decoders and security card, which content is available to the particular subscriber and his equipment (col. 6, lines 55-60). The particular format is not a patentable limitation but rather a design choice.

As per claim 24, Tsuria teaches identifiers of external security modules (6, 8) are grouped in an encrypted list (col.2, lines 29-30).

As per claim 25, Tsuria teaches reception equipment (2) includes a decoder and the external security module (6, 8) includes an access control card (6) in which information about access rights of a subscriber to digital data distributed by an operator is memorized, and in that matching is done between said decoder and said card (6). (col. 2, lines 46-50).

As per claim 26, Tsuria teaches that the reception equipment (2) includes a decoder and the external security module (6, 8) includes a removable security interface (8) provided with a non-volatile memory that can cooperate firstly with the decoder, and secondly with a plurality of conditional access control cards (6) to manage access to digital data distributed by an operator, and in that matching is done between said decoder and said removable security interface (col. 1, lines 55-60 and col. 2, lines 45-55).

As per claim 27, Tsuria teaches the reception equipment (2) includes a decoder provided with a removable security interface (8) with a non-volatile memory that can cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6), and in that matching is done between said removable security interface (8) and said access control cards (col. 2, lines 45-55).

As per claim 28, Tsuria teaches the data are audiovisual programs (col. 1, line 50).

As per claim 29, Tsuria teaches a digital data reception equipment for pairing to one or more external security modules (6, 8) each having an unique identifier [signature] to manage access to digital data distributed by an operator (col. 1, lines 61-65 and col. 3, lines 1-5), comprising means for executing a computer program in a readable medium for:

verifying whether or not the identifier in said external security modules (6, 8) is already memorized in the digital data reception equipment (2) upon connection of said external security modules (6, 8) to the digital data reception equipment [second card is inserted in to the receiver to validate and identify the signature of said second card; col. 7, lines 44-53] ,

activating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier of the external security modules (6, 8) is already memorized in the digital data reception equipment (2) [chaining data; col. 7, lines 45-48] and

deactivating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier in the external security modules (6, 8) is not already memorized in the digital data reception equipment (2) [inherent that if the smart card's signature is not validated, there will be no pairing; col. 7, lines 45-48].

For the record, "a digital data reception equipment for" implies intended use, not functional descriptive material.

As per claim 30, Tsuria teaches it comprises a decoder and in that the external security module (6, 8) is an access control card (6) containing information about access rights of a subscriber to said digital data, matching being done between said decoder and said card (col. 2, lines 45-55).

As per claim 31, Tsuria teaches a decoder and in that the external security module (6, 8) is a removable security interface (8) provided with a non-volatile memory and that is designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6), to manage access to said digital data, matching being done between said decoder and said removable security interface (col. 1, lines 55-60 and col. 2, lines 45-55).

As per claim 32, Tsuria teaches a decoder provided with a removable security interface (8) with a non-volatile memory and that is designed to cooperate firstly with said decoder and secondly with a plurality of conditional access control cards (6) and in that matching is done between said removable security interface (8) and said access control cards (col. 2, lines 45-55).

As per claim 33, Tsuria teaches a decoder that can cooperate with a plurality of external security modules (6, 8) to manage access to audiovisual programs distributed by an operator, each external security module (6, 8) having a unique identifier and including at least one data processing algorithm, with said decoder in comprising means responsive to said processing algorithm for executing orders sent by the operator for:

verifying whether or not the identifier in said external security modules (6, 8)

is already memorized in the digital data reception equipment (2) upon connection of

said external security modules (6, 8) to the digital data reception equipment [second

card is inserted in to the receiver to validate and identify the signature of said second

card; col. 7, lines 44-53] ,

activating the pairing of said digital data reception equipment (2) with said

external security modules (6, 8) if the unique identifier of the external security

modules (6, 8) is already memorized in the digital data reception equipment (2)

[chaining data; col. 7, lines 45-48] and

deactivating the pairing of said digital data reception equipment (2) with said

external security modules (6, 8) if the unique identifier in the external security

modules (6, 8) is not already memorized in the digital data reception equipment (2)

[inherent that if the smart card's signature is not validated, there will be no pairing; col.

7, lines 45-48].

For the record, "a decoder that can" implies intended use, not functional

descriptive material.

As per claim 34, Tsuria teaches external security modules (6, 8) are access

control cards (6) in which information about access rights of a subscriber to digital data

distributed by an operator are stored (col. 2, line 38).

As per claim 35, Tsuria teaches external security modules (6, 8) are removable

security interfaces (8) including a non-volatile memory that can cooperate firstly with the

decoder and secondly with a plurality of conditional access control cards (6) to manage

access to digital data distributed by an operator (col. 6, lines 52-60).

As per claim 36, Tsuria teaches a removable security interface including a non-

volatile memory and designed to cooperate firstly with digital data reception equipment

having a decoder and secondly, having and secondly with a plurality of conditional

access control cards (6), to manage access to digital data distributed by an operator,

each access control card (6) having a unique identifier and containing information about

access rights of a subscriber to said digital data, with said removable security interface

further comprising means for recording the identifier of each access control card in said

non-volatile memory (col. 1, lines 61-65 and col. 3, lines 1-5), and at least one data

processing algorithm for use by said decoder to activate or deactivate the pairing of the

reception equipment to the controls cards (col. 7, lines 44-53).

As per claim 37, Tsuria teaches of a PCMCIA card on which digital data

descrambling software is installed (col. 1, lines 10-15).

As per claim 38, Tsuria teaches consists of a software module (col. 6, lines 50-

54).

As per claim 39, Tsuria teaches an executable computer program stored in a

computer readable medium of a digital data reception equipment (2) that can cooperate

with a plurality of external security modules (6, 8) each having a unique identifier and in

which information about access rights of a subscriber to digital data distributed by an

operator are stored, said digital data reception equipment comprising a computer for

executing said executable computer program includes instructions for:

verifying whether or not the identifier in said external security modules (6, 8)

is already memorized in the digital data reception equipment (2) upon connection of

said external security modules (6, 8) to the digital data reception equipment [second

card is inserted in to the receiver to validate and identify the signature of said second

card; col. 7, lines 44-53] ,

activating the pairing of said digital data reception equipment (2) with said

external security modules (6, 8) if the unique identifier of the external security

modules (6, 8) is already memorized in the digital data reception equipment (2)

[chaining data; col. 7, lines 45-48] and

deactivating the pairing of said digital data reception equipment (2) with said

external security modules (6, 8) if the unique identifier in the external security

modules (6, 8) is not already memorized in the digital data reception equipment (2)

[inherent that if the smart card's signature is not validated, there will be no pairing; col.

7, lines 45-48].

For the record, "an executable computer program ... that can" implies intended

use rather than functional descriptive material.

As per claim 40, Tsuria teaches instructions to locally generate matching control parameters of the reception equipment (2) with an external security module (6, 8) as a function of a signal transmitted to said reception equipment (2) by the operator (col. 6, lines 55-60).

As per claim 41, Tsuria teaches instructions intended to check if the identifier of said external security module (6, 8) is memorized in the reception equipment (2), at each later use of an external security module (6, 8) with the reception equipment (col. 3, lines 15-20).

As per claim 42, Tsuria teaches a system comprising a management platform and a digital data reception equipment (2) connected to services broadcasting network, for communication with the digital data reception equipment and with the digital data reception equipment (2) being paired with a plurality of external security modules (col. 1, lines 61-65 and col. 3, lines 1-5), each having a unique identifier wherein the system further comprises:

a first module arranged in said commercial management platform (1) for generating matching queries (col. 3, lines 15-20),

a second module arranged in said digital data reception equipment (2) that will process the generated queries from the first module to prepare a pairing configuration to control said pairing (col. 3, lines 20-35), using pairing control parameters generated by a computer in said digital data reception equipment based upon [chaining data]

verifying whether or not the identifier in said external security modules (6, 8)

is already memorized in the digital data reception equipment (2) upon connection of

said external security modules (6, 8) to the digital data reception equipment [second

card is inserted in to the receiver to validate and identify the signature of said second

card; col. 7, lines 44-53] ,

activating the pairing of said digital data reception equipment (2) with said

external security modules (6, 8) if the unique identifier of the external security

modules (6, 8) is already memorized in the digital data reception equipment (2)

[chaining data; col. 7, lines 45-48] and

deactivating the pairing of said digital data reception equipment (2) with said

external security modules (6, 8) if the unique identifier in the external security

modules (6, 8) is not already memorized in the digital data reception equipment (2)

[inherent that if the smart card's signature is not validated, there will be no pairing; col.

7, lines 45-48].

As per claim 43, Tsuria teaches said signal is transmitted to a reception

equipment (2) in an EMM message specific to an 25 external security module (6, 8)

associated with this reception equipment (col. 6, lines 55-60).

As per claim 44, Tsuria teaches a signal is transmitted to a reception equipment

(2) in an EMM message specific to this reception equipment (col. 6, lines 55-60).

As per claim 45, Tsuria teaches a signal is transmitted to a group of reception equipment (2) in an EMM message specific to a group of external security modules (6, 8) associated with said reception equipment (col. 6, lines 55-60).

As per claim 46, Tsuria teaches signal is transmitted to a group of reception equipment (2) in an EMM message specific to said group of reception equipment (col. 6, lines 55-60).

As per claim 47, Tsuria teaches said check signal is transmitted in a private flow processed by a dedicated software executable in each reception equipment as a function of the identifier of the external security module associated with said reception equipment (col. 6, lines 55-60).

As per claims 48-53, Tsuria teaches EMM are formatted to convey to the decoders and security card, which content is available to the particular subscriber and his equipment (col. 6, lines 55-60). The particular format is not a patentable limitation but rather a design choice.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax

phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431